Cyberkriminelle missbrauchen Ihre Daten und Emotionen

Verstehen wie Kriminelle Sie heutzutage angreifen

Social Engineering ist eine der häufigsten Methoden, mit denen Cyberkriminelle in Unternehmen einbrechen – ohne Computer zu hacken. Stattdessen nehmen sie Menschen ins Visier. Indem sie sich als vertrauenswürdige Personen ausgeben, bringen Angreifende Mitarbeitende dazu, sensible Informationen preiszugeben oder Handlungen auszuführen, die weitere Angriffe ermöglichen. Dies kann schwerwiegende Folgen haben: Datendiebstahl, finanzieller Verlust, Rufschädigung oder sogar der vollständige Bankrott. Der erste Schritt sich zu schützen ist zu verstehen, wie Social Engineering funktioniert.

Wie funktioniert Social Engineering?

Der Social-Engineering-Angriffszyklus umfasst **vier Phasen**:

1. Informationsbeschaffung

Angreifende sammeln persönliche und organisatorische Daten aus sozialen Medien und von Webseiten – automatisierte Tools machen dies schnell und einfach.

2. Beziehungen aufbauen, Vertrauen schaffen

Sie nutzen die gesammelten Informationen, um sich als Kollegin, Partner, Lieferanten oder Expertin auszugeben – und gewinnen so durch E-Mails, Anrufe, Chats oder sogar persönliche Treffen das Vertrauen ihrer Opfer.

3. Ausnutzen

Sobald das Vertrauen gewonnen ist, können Angreifende Opfer dazu verleiten oder unter Druck setzen, Zugangsdaten weiterzugeben, Zugang zu einem gesperrten Bereich zu gewähren oder Geld zu überweisen – ohne Verdacht zu erregen.

4. Ausführen

Mit dem erlangten Zugriff handeln Angreifende unbemerkt: Sie stehlen Daten, spionieren über Webcams, verschlüsseln Dateien, um Lösegeld zu erpressen, oder manipulieren Systeme. Der Schaden kann enorm sein – oft bevor überhaupt bemerkt wird, dass etwas nicht stimmt.

Erkennen

- Aus heiterem Himmel ungewöhnliche oder dringende Anfragen, insbesondere in Bezug auf Geld oder Daten.
- Anrufe oder Nachrichten, die Sie zu schnellem Handeln oder zum Umgehen von Vorschriften auffordern, um jemandem in einer dringenden Situation zu helfen.
- Jemand gibt sich als interner Mitarbeiter aus, verwendet jedoch externe E-Mail-Adressen.

Was können Sie tun?

- **Seien Sie vorsichtig mit dem, was Sie preisgeben:** Ihre beruflichen Erfolge, Urlaubsfotos oder Ihr Lieblingscafé mögen harmlos erscheinen – zusammen genommen machen sie es Angreifern jedoch leicht, überzeugend zu wirken. Das Internet weiss oft mehr über Sie als Ihre Freunde.
- **Überprüfen Sie die Angaben über einen anderen Kanal:** Wenn Sie eine seltsame Nachricht erhalten, wie z. B. „Können Sie diese dringende Rechnung genehmigen?“, überprüfen Sie diese über eine bekannte Telefonnummer oder persönlich – nicht einfach durch eine Antwort im gleichen Medium.
- **Halten Sie inne, bevor Sie handeln:** Social Engineers erzeugen Druck. Wenn Ihnen etwas seltsam oder zu gut erscheint, um wahr zu sein, nehmen Sie sich einen Moment Zeit – und melden Sie es Ihrem IT-Team oder Sicherheitsbeauftragten.

Erfahren Sie mehr

🔗 Cyberkriminalität für Einsteiger – Teil 1: Wie viel kann Granny Smith über Sie herausfinden?

Aus einzelnen Informationsschnipseln lässt sich mit wenig Aufwand ein detailliertes Bild von uns erstellen. Diese Informationen können Cyberkriminelle nutzen, um gezielte Angriffe auf uns zu starten. Welche Daten geben Sie preis?

GÉANT